

# **EXHIBIT A**

**Excerpts of SW-SEC00259782**



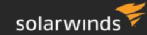
## MONTHLY IT LEADERSHIP MEETING

CONFIDENTIAL

DEVELOPMENT OPERATIONS & INFORMATION TECHNOLOGY (DOIT)

**A PROACTIVE SECURITY MODEL**

- \$660K INVESTMENT REQUEST. ACCELERATION OPPORTUNITY

**Budget Request**

Description	Annual \$
Security Program Manager	\$180
Security Analyst	\$180
Application Firewall	\$40
Internal/External PEN test	\$100
Security Training	\$30
Secure Development Training	\$30
Commercial application code scanners	\$100
<b>Total</b>	<b>\$660</b>

**Risk of Non-Investment**

- Current state of security leaves us in a very **vulnerable state** for our critical assets. A compromise of these assets would **damage our reputation and impact us financially**.
- Lack of cyber hygiene leaves us **open to being a target** of opportunity and a compromise will create downtime and lost revenue
- We have had **28 logged security incidents** this year to date. Reactive responses costs significantly more than being proactive.
- We have **lost a renewal** of DPA for Accenture (192K) due to utilizing free code scanning tools that did not find all vulnerabilities.
- Without training our **employees** will continue to be one of our **biggest risks**
- Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in **qualifying questionnaires**. Without appropriate answers we will lose business

7